OFFICE OF THE CHIEF OF POLICE

SPECIAL ORDER NO. 2 February 2, 2017

APPROVED BY THE BOARD OF POLICE COMMISSIONERS ON JANUARY 10, 2017

SUBJECT: CELLULAR COMMUNICATIONS INTERCEPTION TECHNOLOGY USE AND DEPLOYMENT - ESTABLISHED

BACKGROUND: Cellular communications interception technology provides valuable assistance in support of important public safety objectives when deployed as part of a criminal apprehension effort, and in emergency situations to locate at-risk persons or missing children. As with any law enforcement capability, this technology must be used in a manner consistent with the requirements and protections of the Constitution and all applicable statutory authorities. Moreover, any information obtained from the use of cellular communications interception technology must be handled in accordance with applicable statutes, regulations, and policies that guide law enforcement in its collection, retention, and disclosure of data. As set forth in greater detail below, this technology may be utilized only after a search warrant has been secured, or where an "emergency" exists (as defined in California Penal Code Section 1546.1), following approval for such emergency deployment by the Commanding Officer, Counter-Terrorism and Special Operations Bureau (CTSOB), or in his or her absence, the Commanding Officer, Detective Bureau (DB). This Manual Section is established in accordance with California Government Code Section 53166.

PURPOSE: This Order establishes Department Manual Section 3/568.55, *Cellular Communications Interception Technology Use and Deployment.*

PROCEDURE: Department Manual Section 3/568.55, *Cellular Communications Interception Technology Use and Deployment,* has been established and is attached.

AMENDMENT: This Order adds Section 3/568.55 to the Department Manual.

AUDIT RESPONSIBILITY: The Commanding Officer, Audit Division, shall review this directive and determine whether an audit or inspection shall be conducted in accordance with Department Manual Section 0/080.30.

CHARLIE BECK
Chief of Police

Attachment

DISTRIBUTION "D"

DEPARTMENT MANUAL
VOLUME III
Established by Special Order No. 2, 2017

568.55 CELLULAR COMMUNICATIONS INTERCEPTION TECHNOLOGY USE AND DEPLOYMENT. *Cellular communications interception technology provides valuable assistance in support of important public safety objectives when deployed as part of a criminal apprehension effort, and in emergency situations to locate at-risk persons or missing children. As with any law enforcement capability, this technology must be used in a manner consistent with the requirements and protections of the Constitution and all applicable statutory authorities. Information obtained from the use of cellular communications interception technology shall be handled in accordance with applicable statutes, regulations, and policies that guide law enforcement in its collection, retention, and disclosure of data.*

Authorized Personnel and Uses of Cellular Communications Interception Technology. *Only sworn personnel assigned to Major Crimes Division (MCD) are authorized to use cellular communications interception technology and shall maintain custody and control over all such devices.*

Major Crimes Division sworn personnel shall:

- *Oversee and approve all non-emergency requests for deployment of the technology made by members of the Department, who may then have access to information obtained via such deployment; and,*
- *All deployments of cellular communications interception technology by MCD shall receive prior approval from the Commanding Officer (CO), MCD [when the CO, MCD, is unavailable, approval for the deployment of this technology shall default to the CO, Counter-Terrorism and Special Operations Bureau (CTSOB)].*

  Note: *A lieutenant who is "acting" for the CO, MCD, shall not be permitted to grant approval for use of this technology.*

Cellular communications interception technology may be deployed for the following:

- *Criminal investigations; or,*
- *Emergency situations to locate at-risk persons or missing children, as defined in California Penal Code (PC) Section 1546.1.*

This technology shall be utilized only for these purposes and when either authorized by a warrant signed by a judicial officer prior to deployment or when an emergency exists involving the danger of death or serious physical injury to an individual.

> ***Note:*** *Deployment pursuant to an emergency shall require prior approval of the CO, CTSOB, or in his or her absence, the CO, Detective Bureau, and shall adhere to all requirements set forth in PC Section 1546, et seq.*

All Department personnel authorized to use cellular communications interception technology shall:

- *Receive training, to include training on privacy and civil liberties, by a qualified MCD component or expert; and,*
- *Be supervised to ensure the proper use of the technology.*

Note: *Non-MCD Department personnel or non-Department individuals who may have received outside training on the general use of such technology shall not be permitted to engage in any use of the technology in the Department's possession.*

Legal Process for Use of Cellular Communications Interception Technology. *Authorized Department personnel using cellular communications interception technology shall do so only pursuant to a lawfully issued search warrant. However, in the case of an emergency involving danger of death or serious physical injury, deployment may occur without prior judicial authorization, so long as Department personnel file an application for a search warrant or court order within three days following its deployment [pursuant to PC Section 1546.1 (h)].*

Warrant applications shall contain all information required under PC Sections 1524, 1534, and 1546.1(d), and shall accurately describe the underlying purpose and activities for which an order or authorization is sought. The application or supporting affidavit shall:

- *Describe in general terms the technique to be employed. The description should indicate that investigators plan to send signals to the cellular telephone that shall cause that phone, and non-target cellular telephones on the same provider network in close physical proximity, to emit unique identifiers which will be acknowledged by the technology. It shall further provide that investigators will use the information identified to determine the physical location of the target cellular device;*
- *Inform the court that the target cellular device (e.g., cell phone) and other cellular devices in the area might experience a temporary interruption of service from the service provider. The application shall also note that any potential service interruption to non-target devices would be temporary and all operations will be conducted to ensure a minimal amount of interference to non-target devices; and,*
- *Inform the court about how law enforcement is incapable of retaining any numerical or other information not associated with the target cellular device, and that at no time is the use of this technology meant for the collection of non-targeted information. The application shall also state that law enforcement will not intentionally use any non-target information, except to identify and distinguish the target device from other devices.*

Requirements for Shared Use of Cellular Communications Interception Technology or Information Derived from Such Use. *Department personnel, as well as outside partner law enforcement agencies, may request the use of cellular communications interception technology to aid in locating cellular devices whose unique identifiers are already known to law enforcement. Use of the technology and any information derived therefrom shall be restricted to criminal investigations, or in emergency situations to locate at-risk persons or missing children.*

The Department shall not share use of the device or any information obtained from its use with any other local agency [as defined in California Government Code Section 53166(a)(2)] until the Department enters into a memorandum of understanding (MOU) or other agreement with each requesting local agency regarding the shared use of the technology. The terms of each MOU shall be consistent with this policy.

The Department shall seek an MOU with any requesting law enforcement agency prior to deployment of this technology for law enforcement purposes, wherein all partner agencies shall be clearly identified. All non-Departmental requests for assistance involving deployment of the technology shall be in writing, either electronic or print. The resulting information (i.e., location data related to the targeted device) provided to authorized partner agencies shall be released only pursuant to the review and approval of the CO, CTSOB, as established in the MOU entered into with a partner agency.

Monitoring and Auditing of Use of Cellular Communications Interception Technology; Limitations on Retention of Information. *Department personnel shall not collect, retain or disseminate any data from the deployment of cellular communications interception technology except as authorized by this Manual section and by law.*

The following shall apply to data management.

- *When the equipment is used to locate a known cellular device, all data shall be deleted from the cell-site simulator as soon as the investigation has been completed. Importantly, the data referenced above (relevant to location) consists solely of identifiers [i.e., International Mobile Subscriber Identity (IMSI), Mobile Identification Number (MIN)] related to the targeted device, and the location of the device as indicated by the cell-site simulator. This information is usable only for locating the targeted device, and shall have no application outside this purpose;*
- *Upon completion of a mission involving the use of a cell-site simulator, MCD supervision shall be responsible for ensuring that the procedures for the purging of mission-related information were followed properly (in accordance with this Manual section and California Government Code Section 53166); and,*
- *Major Crimes Division shall utilize an inspection/audit program to ensure that the cellular communications interception technology is utilized according to the terms of this policy; including management of any information (retention/destruction), the temporal and substantive requirements for obtaining a search warrant/court order, and other requirements set forth in PC Section 1546, et seq.*

Employee Accountability. *All sworn MCD personnel authorized to use cellular communications interception technology shall be provided with a copy of this Department Manual section and receive specialized training in the use of this technology. Periodic review of this Department Manual section and training concerning use of the technology (e.g., significant advances in technological capabilities, type of information collected, and/or the manner in which it was collected) shall be the responsibility of MCD.*